312-49v10 Dumps

Computer Hacking Forensic Investigator (CHFI-v10)

https://www.certleader.com/312-49v10-dumps.html

NEW QUESTION 1
- (Exam Topic 1)
You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. Airsnort
B. Snort
C. Ettercap
D. RaidSniff

Answer: C

NEW QUESTION 2
- (Exam Topic 1)
While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?

A. Keep the information of file for later review
B. Destroy the evidence
C. Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge
D. Present the evidence to the defense attorney

Answer: C

NEW QUESTION 3
- (Exam Topic 1)
George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used.
What IDS feature must George implement to meet this requirement?

A. Signature-based anomaly detection
B. Pattern matching
C. Real-time anomaly detection
D. Statistical-based anomaly detection

Answer: C

NEW QUESTION 4
- (Exam Topic 1)
What operating system would respond to the following command?

A. Windows 95
B. FreeBSD
C. Windows XP
D. Mac OS X

Answer: B

NEW QUESTION 5
- (Exam Topic 1)
You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

A. The registry
B. The swap file
C. The recycle bin
D. The metadata

Answer: B

NEW QUESTION 6
- (Exam Topic 1)
In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

A. one who has NTFS 4 or 5 partitions
B. one who uses dynamic swap file capability
C. one who uses hard disk writes on IRQ 13 and 21
D. one who has lots of allocation units per block or cluster

Answer: D

NEW QUESTION 7

- (Exam Topic 1)
Law enforcement officers are conducting a legal search for which a valid warrant was obtained.
While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?

A. Plain view doctrine
B. Corpus delicti
C. Locard Exchange Principle
D. Ex Parte Order

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

A. Stateful firewalls do not work with packet filtering firewalls
B. NAT does not work with stateful firewalls
C. IPSEC does not work with packet filtering firewalls
D. NAT does not work with IPSEC

Answer: D

NEW QUESTION 9
- (Exam Topic 1)
What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

A. Cached password hashes for the past 20 users
B. Service account passwords in plain text
C. IAS account names and passwords
D. Local store PKI Kerberos certificates

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately.
Which organization coordinates computer crimes investigations throughout the United States?

A. Internet Fraud Complaint Center
B. Local or national office of the U.
C. Secret Service
D. National Infrastructure Protection Center
E. CERT Coordination Center

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
Area density refers to:

A. the amount of data per disk
B. the amount of data per partition
C. the amount of data per square inch
D. the amount of data per platter

Answer: A

NEW QUESTION 13
- (Exam Topic 1)
When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS
B. Active IDS
C. Progressive IDS
D. NIPS

Answer: B

NEW QUESTION 16
- (Exam Topic 1)
A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation. During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible

suspects including three summer interns. Where did the incident team go wrong?

A. They examined the actual evidence on an unrelated system
B. They attempted to implicate personnel without proof
C. They tampered with evidence by using it
D. They called in the FBI without correlating with the fingerprint data

Answer: C

NEW QUESTION 18
- (Exam Topic 1)
Corporate investigations are typically easier than public investigations because:

A. the users have standard corporate equipment and software
B. the investigator does not have to get a warrant
C. the investigator has to get a warrant
D. the users can load whatever they want on their machines

Answer: B

NEW QUESTION 19
- (Exam Topic 1)
When reviewing web logs, you see an entry for resource not found in the HTTP status code filed. What is the actual error code that you would see in the log for resource not found?

A. 202
B. 404
C. 505
D. 909

Answer: B

NEW QUESTION 22
- (Exam Topic 1)
You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacture. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?

A. the attorney-work-product rule
B. Good manners
C. Trade secrets
D. ISO 17799

Answer: A

NEW QUESTION 25
- (Exam Topic 2)
Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish?
dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync

A. Fill the disk with zeros
B. Low-level format
C. Fill the disk with 4096 zeros
D. Copy files from the master disk to the slave disk on the secondary IDE controller

Answer: A

NEW QUESTION 27
- (Exam Topic 2)
Which of the following file contains the traces of the applications installed, run, or uninstalled from a system?

A. Shortcut Files
B. Virtual files
C. Prefetch Files
D. Image Files

Answer: A

NEW QUESTION 31
- (Exam Topic 2)
When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

A. One
B. Two
C. Three
D. Four

Answer: B

NEW QUESTION 36
- (Exam Topic 2)
Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

A. Three
B. One
C. Two
D. Four

Answer: B

NEW QUESTION 37
- (Exam Topic 2)
What type of attack sends SYN requests to a target system with spoofed IP addresses?

A. SYN flood
B. Ping of death
C. Cross site scripting
D. Land

Answer: A

NEW QUESTION 38
- (Exam Topic 2)
Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?

A. Net config
B. Net file
C. Net share
D. Net sessions

Answer: B

NEW QUESTION 42
- (Exam Topic 2)
To check for POP3 traffic using Ethereal, what port should an investigator search by?

A. 143
B. 25
C. 110
D. 125

Answer: C

NEW QUESTION 44
- (Exam Topic 2)
When using an iPod and the host computer is running Windows, what file system will be used?

A. iPod+
B. HFS
C. FAT16
D. FAT32

Answer: D

NEW QUESTION 45
- (Exam Topic 1)
From the following spam mail header, identify the host IP that sent this spam? From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001
Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk (8.11.6/8.11.6) with ESMTP id
fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)
Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1)
with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)
Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk From: "china hotel web"
To: "Shlam"
Subject: SHANGHAI (HILTON HOTEL) PACKAGE
Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0
X- Priority: 3 X-MSMail- Priority: Normal
Reply-To: "china hotel web"

A. 137.189.96.52
B. 8.12.1.0
C. 203.218.39.20
D. 203.218.39.50

Answer: C

NEW QUESTION 49
- (Exam Topic 1)
What binary coding is used most often for e-mail purposes?

A. MIME
B. Uuencode
C. IMAP
D. SMTP

Answer: A

NEW QUESTION 53
- (Exam Topic 1)
Software firewalls work at which layer of the OSI model?

A. Application
B. Network
C. Transport
D. Data Link

Answer: D

NEW QUESTION 55
- (Exam Topic 1)
Lance wants to place a honeypot on his network. Which of the following would be your recommendations?

A. Use a system that has a dynamic addressing on the network
B. Use a system that is not directly interacting with the router
C. Use it on a system in an external DMZ in front of the firewall
D. It doesn't matter as all replies are faked

Answer: D

NEW QUESTION 56
- (Exam Topic 1)
After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

A. Enable direct broadcasts
B. Disable direct broadcasts
C. Disable BGP
D. Enable BGP

Answer: B

NEW QUESTION 59
- (Exam Topic 1)
What will the following command accomplish?

A. Test ability of a router to handle over-sized packets
B. Test the ability of a router to handle under-sized packets
C. Test the ability of a WLAN to handle fragmented packets
D. Test the ability of a router to handle fragmented packets

Answer: A

NEW QUESTION 60
- (Exam Topic 1)
You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls? (Choose two.)

A. 162
B. 161
C. 163
D. 160

Answer: AB

NEW QUESTION 63
- (Exam Topic 1)
In a FAT32 system, a 123 KB file will use how many sectors?

A. 34
B. 25
C. 11
D. 56

Answer:

B

NEW QUESTION 65
- (Exam Topic 1)
What does ICMP Type 3/Code 13 mean?

A. Host Unreachable
B. Administratively Blocked
C. Port Unreachable
D. Protocol Unreachable

Answer: B

NEW QUESTION 66
- (Exam Topic 1)
You are working as Computer Forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firm's employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?

A. Inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned
B. Inform the owner that conducting an investigation without a policy is a violation of the 4th amendment
C. Inform the owner that conducting an investigation without a policy is a violation of the employee's expectation of privacy
D. Inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies

Answer: C

NEW QUESTION 67
- (Exam Topic 1)
Which of the following is NOT a graphics file?

A. Picture1.tga
B. Picture2.bmp
C. Picture3.nfo
D. Picture4.psd

Answer: C

NEW QUESTION 71
- (Exam Topic 1)
You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Packet filtering firewall
B. Circuit-level proxy firewall
C. Application-level proxy firewall
D. Stateful firewall

Answer: D

NEW QUESTION 75
- (Exam Topic 1)
What should you do when approached by a reporter about a case that you are working on or have worked on?

A. Refer the reporter to the attorney that retained you
B. Say, "no comment"
C. Answer all the reporter's questions as completely as possible
D. Answer only the questions that help your case

Answer: A

NEW QUESTION 76
- (Exam Topic 1)
In Microsoft file structures, sectors are grouped together to form:

A. Clusters
B. Drives
C. Bitstreams
D. Partitions

Answer: A

NEW QUESTION 77
- (Exam Topic 1)
If you plan to startup a suspect's computer, you must modify the to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.

A. deltree command
B. CMOS
C. Boot.sys
D. Scandisk utility

Answer: C

NEW QUESTION 78
- (Exam Topic 1)
You are running through a series of tests on your network to check for any security vulnerabilities.
After normal working hours, you initiate a DoS attack against your external firewall. The firewall Quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A. The firewall failed-bypass
B. The firewall failed-closed
C. The firewall ACL has been purged
D. The firewall failed-open

Answer: D

NEW QUESTION 81
- (Exam Topic 1)
Item 2If you come across a sheepdip machine at your client site, what would you infer?

A. A sheepdip coordinates several honeypots
B. A sheepdip computer is another name for a honeypot
C. A sheepdip computer is used only for virus-checking.
D. A sheepdip computer defers a denial of service attack

Answer: C

NEW QUESTION 85
- (Exam Topic 1)
When conducting computer forensic analysis, you must guard against So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

A. Hard Drive Failure
B. Scope Creep
C. Unauthorized expenses
D. Overzealous marketing

Answer: B

NEW QUESTION 88
- (Exam Topic 1)
What happens when a file is deleted by a Microsoft operating system using the FAT file system?

A. only the reference to the file is removed from the FAT
B. the file is erased and cannot be recovered
C. a copy of the file is stored and the original file is erased
D. the file is erased but can be recovered

Answer: A

NEW QUESTION 93
- (Exam Topic 1)
When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

A. Recycle Bin
B. MSDOS.sys
C. BIOS
D. Case files

Answer: A

NEW QUESTION 94
- (Exam Topic 1)
In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

A. rules of evidence
B. law of probability
C. chain of custody
D. policy of separation

Answer: C

NEW QUESTION 98
- (Exam Topic 1)
Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. Tracert
B. Smurf scan
C. Ping trace
D. ICMP ping sweep

Answer: D

NEW QUESTION 100
- (Exam Topic 1)
George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network.
What filter should George use in Ethereal?

A. src port 23 and dst port 23
B. udp port 22 and host 172.16.28.1/24
C. net port 22
D. src port 22 and dst port 22

Answer: D

NEW QUESTION 104
- (Exam Topic 1)
What does the acronym POST mean as it relates to a PC?

A. Primary Operations Short Test
B. PowerOn Self Test
C. Pre Operational Situation Test
D. Primary Operating System Test

Answer: B

NEW QUESTION 105
- (Exam Topic 1)
_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

A. Network Forensics
B. Computer Forensics
C. Incident Response
D. Event Reaction

Answer: B

NEW QUESTION 107
- (Exam Topic 1)
Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security.
Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

A. Border Gateway Protocol
B. Cisco Discovery Protocol
C. Broadcast System Protocol
D. Simple Network Management Protocol

Answer: B

NEW QUESTION 111
- (Exam Topic 1)
As a security analyst, you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

A. The IP address of the employees' computers
B. Bank account numbers and the corresponding routing numbers
C. The employees network usernames and passwords
D. The MAC address of the employees' computers

Answer: C

NEW QUESTION 114
- (Exam Topic 1)
The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

A. Any data not yet flushed to the system will be lost
B. All running processes will be lost
C. The /tmp directory will be flushed
D. Power interruption will corrupt the pagefile

Answer: A

NEW QUESTION 117
- (Exam Topic 1)
Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

A. ATM
B. UDP
C. BPG
D. OSPF

Answer: D

NEW QUESTION 119
- (Exam Topic 1)
You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records
B. Enumerate MX and A records from DNS
C. Establish a remote connection to the Domain Controller
D. Enumerate domain user accounts and built-in groups

Answer: D

NEW QUESTION 122
- (Exam Topic 1)
Why is it a good idea to perform a penetration test from the inside?

A. It is never a good idea to perform a penetration test from the inside
B. Because 70% of attacks are from inside the organization
C. To attack a network from a hacker's perspective
D. It is easier to hack from the inside

Answer: B

NEW QUESTION 127
- (Exam Topic 1)
Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

A. Use VMware to be able to capture the data in memory and examine it
B. Give the Operating System a minimal amount of memory, forcing it to use a swap file
C. Create a Separate partition of several hundred megabytes and place the swap file there
D. Use intrusion forensic techniques to study memory resident infections

Answer: C

NEW QUESTION 128
- (Exam Topic 1)
You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so Quickly?

A. Passwords of 14 characters or less are broken up into two 7-character hashes
B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network
C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty
D. The passwords that were cracked are local accounts on the Domain Controller

Answer: A

NEW QUESTION 129
- (Exam Topic 1)
In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?

A. evidence must be handled in the same way regardless of the type of case
B. evidence procedures are not important unless you work for a law enforcement agency
C. evidence in a criminal case must be secured more tightly than in a civil case
D. evidence in a civil case must be secured more tightly than in a criminal case

Answer: C

NEW QUESTION 131
- (Exam Topic 1)
You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years.
You navigate to archive. org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?

A. Web bug
B. CGI code
C. Trojan.downloader
D. Blind bug

Answer: A

NEW QUESTION 132
- (Exam Topic 1)
When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts in the first letter position of the filename in the FAT database.

A. A Capital X
B. A Blank Space
C. The Underscore Symbol
D. The lowercase Greek Letter Sigma (s)

Answer: D

NEW QUESTION 135
- (Exam Topic 1)
E- mail logs contain which of the following information to help you in your investigation? (Choose four.)

A. user account that was used to send the account
B. attachments sent with the e-mail message
C. unique message identifier
D. contents of the e-mail message
E. date and time the message was sent

Answer: ACDE

NEW QUESTION 138
- (Exam Topic 1)
In Linux, what is the smallest possible shellcode?

A. 24 bytes
B. 8 bytes
C. 800 bytes
D. 80 bytes

Answer: A

NEW QUESTION 141
- (Exam Topic 1)
The efforts to obtain information before a trail by demanding documents, depositions, questioned and answers written under oath, written requests for admissions of fact and examination of the scene is a description of what legal term?

A. Detection
B. Hearsay
C. Spoliation
D. Discovery

Answer: D

NEW QUESTION 146
- (Exam Topic 1)
With Regard to using an Antivirus scanner during a computer forensics investigation, You should:

A. Scan the suspect hard drive before beginning an investigation
B. Never run a scan on your forensics workstation because it could change your systems configuration
C. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
D. Scan your Forensics workstation before beginning an investigation

Answer: D

NEW QUESTION 147

- (Exam Topic 1)
You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation.
Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?

A. All forms should be placed in an approved secure container because they are now primary evidence in the case.
B. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.
C. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file.
D. All forms should be placed in the report file because they are now primary evidence in the case.

Answer: B

NEW QUESTION 149
- (Exam Topic 1)
Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies?
What type of Penetration Testing is Larry planning to carry out?

A. Router Penetration Testing
B. DoS Penetration Testing
C. Firewall Penetration Testing
D. Internal Penetration Testing

Answer: B

NEW QUESTION 153
- (Exam Topic 1)
How many bits is Source Port Number in TCP Header packet?

A. 16
B. 32
C. 48
D. 64

Answer: A

NEW QUESTION 156
- (Exam Topic 1)
Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search.
link:www.ghttech.net What will this search produce?

A. All sites that ghttech.net links to
B. All sites that link to ghttech.net
C. All search engines that link to .net domains
D. Sites that contain the code: link:www.ghttech.net

Answer: B

NEW QUESTION 161
- (Exam Topic 1)
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Polymorphic
B. Metamorphic
C. Oligomorhic
D. Transmorphic

Answer: B

NEW QUESTION 165
- (Exam Topic 1)
To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

A. Computer Forensics Tools and Validation Committee (CFTVC)
B. Association of Computer Forensics Software Manufactures (ACFSM)
C. National Institute of Standards and Technology (NIST)
D. Society for Valid Forensics Tools and Testing (SVFTT)

Answer: C

NEW QUESTION 170
- (Exam Topic 1)
If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?

A. The system files have been copied by a remote attacker
B. The system administrator has created an incremental backup
C. The system has been compromised using a t0rnrootkit
D. Nothing in particular as these can be operational files

Answer: D

NEW QUESTION 174
- (Exam Topic 1)
During the course of a corporate investigation, you find that an Employee is committing a crime. Can the Employer file a criminal complaint with Police?

A. Yes, and all evidence can be turned over to the police
B. Yes, but only if you turn the evidence over to a federal law enforcement agency
C. No, because the investigation was conducted without following standard police procedures
D. No, because the investigation was conducted without warrant

Answer: A

NEW QUESTION 177
- (Exam Topic 1)
Which is a standard procedure to perform during all computer forensics investigations?

A. with the hard drive removed from the suspect PC, check the date and time in the system's CMOS
B. with the hard drive in the suspect PC, check the date and time in the File Allocation Table
C. with the hard drive removed from the suspect PC, check the date and time in the system's RAM
D. with the hard drive in the suspect PC, check the date and time in the system's CMOS

Answer: A

NEW QUESTION 178
- (Exam Topic 1)
Microsoft Outlook maintains email messages in a proprietary format in what type of file?

A. .email
B. .mail
C. .pst
D. .doc

Answer: C

NEW QUESTION 179
- (Exam Topic 1)
In General, Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.

A. Network Forensics
B. Data Recovery
C. Disaster Recovery
D. Computer Forensics

Answer: D

NEW QUESTION 183
- (Exam Topic 1)
When you carve an image, recovering the image depends on which of the following skills?

A. Recognizing the pattern of the header content
B. Recovering the image from a tape backup
C. Recognizing the pattern of a corrupt file
D. Recovering the image from the tape backup

Answer: A

NEW QUESTION 187
- (Exam Topic 1)
You are working for a local police department that services a population of 1,000,000 people and you have been given the task of building a computer forensics lab. How many law-enforcement computer investigators should you request to staff the lab?

A. 8
B. 1
C. 4
D. 2

Answer: C

NEW QUESTION 188
- (Exam Topic 1)
The police believe that Melvin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers and Educational Institutions. They also suspect that he has been stealing, copying and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspects door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

A. The Fourth Amendment
B. The USA patriot Act
C. The Good Samaritan Laws
D. The Federal Rules of Evidence

Answer: A

NEW QUESTION 191
- (Exam Topic 1)
How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

A. 128
B. 64
C. 32
D. 16

Answer: C

NEW QUESTION 192
- (Exam Topic 1)
When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:

A. Automate Collection from image files
B. Avoiding copying data from the boot partition
C. Acquire data from host-protected area on a disk
D. Prevent Contamination to the evidence drive

Answer: D

NEW QUESTION 197
- (Exam Topic 1)
You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. allinurl:"exchange/logon.asp"
B. intitle:"exchange server"
C. locate:"logon page"
D. outlook:"search"

Answer: A

NEW QUESTION 199
- (Exam Topic 1)
Bob has been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the System for a period of three weeks. However, law enforcement agencies were recoding his every activity and this was later presented as evidence.
The organization had used a Virtual Environment to trap Bob. What is a Virtual Environment?

A. A Honeypot that traps hackers
B. A system Using Trojaned commands
C. An environment set up after the user logs in
D. An environment set up before a user logs in

Answer: A

NEW QUESTION 200
- (Exam Topic 1)
Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?

A. Sector
B. Metadata
C. MFT
D. Slack Space

Answer: D

NEW QUESTION 205
- (Exam Topic 1)

Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?

A. 18 U.S.
B. 1029
C. 18 U.S.
D. 1362
E. 18 U.S.
F. 2511
G. 18 U.S.
H. 2703

Answer: A

NEW QUESTION 208
- (Exam Topic 1)
This is original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.

A. Master Boot Record (MBR)
B. Master File Table (MFT)
C. File Allocation Table (FAT)
D. Disk Operating System (DOS)

Answer: C

NEW QUESTION 209
- (Exam Topic 1)
Sectors in hard disks typically contain how many bytes?

A. 256
B. 512
C. 1024
D. 2048

Answer: B

NEW QUESTION 212
- (Exam Topic 1)
Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.
The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. False negatives
B. False positives
C. True negatives
D. True positives

Answer: A

NEW QUESTION 214
- (Exam Topic 1)
When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

A. Universal Time Set
B. Network Time Protocol
C. SyncTime Service
D. Time-Sync Protocol

Answer: B

NEW QUESTION 216
- (Exam Topic 1)
What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

A. ICMP header field
B. TCP header field
C. IP header field
D. UDP header field

Answer: B

NEW QUESTION 217
- (Exam Topic 1)
You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of

the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

A. Microsoft Methodology
B. Google Methodology
C. IBM Methodology
D. LPT Methodology

Answer: D

NEW QUESTION 220
- (Exam Topic 4)
This law sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.

A. The CAN-SPAM act
B. Federal Spam act
C. Telemarketing act
D. European Anti-Spam act

Answer: A

NEW QUESTION 224
- (Exam Topic 4)
According to RFC 3227, which of the following is considered as the most volatile item on a typical system?

A. Registers and cache
B. Temporary system files
C. Archival media
D. Kernel statistics and memory

Answer: A

NEW QUESTION 225
- (Exam Topic 4)
To which phase of the computer forensics investigation process does "planning and budgeting of a forensics lab" belong?

A. Post-investigation phase
B. Reporting phase
C. Pre-investigation phase
D. Investigation phase

Answer: C

NEW QUESTION 230
- (Exam Topic 4)
Mark works for a government agency as a cyber-forensic investigator. He has been given the task of restoring data from a hard drive. The partition of the hard drive was deleted by a disgruntled employee In order to hide their nefarious actions. What tool should Mark use to restore the data?

A. EFSDump
B. Diskmon D
C. iskvlew
D. R-Studio

Answer: D

NEW QUESTION 235
- (Exam Topic 4)
An investigator Is examining a file to identify any potentially malicious content. To avoid code execution and still be able to uncover hidden indicators of compromise (IOC), which type of examination should the investigator perform:

A. Threat hunting
B. Threat analysis
C. Static analysis
D. Dynamic analysis

Answer: B

NEW QUESTION 237
- (Exam Topic 4)
During an Investigation. Noel found a SIM card from the suspect's mobile. The ICCID on the card is 8944245252001451548.
What does the first four digits (89 and 44) In the ICCID represent?

A. TAC and industry identifier
B. Country code and industry identifier
C. Industry identifier and country code
D. Issuer identifier number and TAC

Answer: C

NEW QUESTION 238
- (Exam Topic 4)
Which of the following tools will allow a forensic Investigator to acquire the memory dump of a suspect machine so that It may be Investigated on a forensic workstation to collect evidentiary data like processes and Tor browser artifacts?

A. DB Browser SQLite
B. Bulk Extractor
C. Belkasoft Live RAM Capturer and AccessData FTK imager
D. Hex Editor

Answer: C

NEW QUESTION 239
- (Exam Topic 4)
Consider a scenario where a forensic investigator is performing malware analysis on a memory dump acquired from a victims computer. The investigator uses Volatility Framework to analyze RAM contents; which plugin helps investigator to identify hidden processes or injected code/DLL in the memory dump?

A. pslist
B. malscan
C. mallist
D. malfind

Answer: D

NEW QUESTION 240
- (Exam Topic 4)
Which of the following statements is true with respect to SSDs (solid-state drives)?

A. Like HDD
B. SSDs also have moving parts
C. SSDs cannot store non-volatile data
D. SSDs contain tracks, clusters, and sectors to store data
E. Faster data access, lower power usage, and higher reliability are some of the m<ijor advantages of SSDs over HDDs

Answer: D

NEW QUESTION 245
- (Exam Topic 4)
In Java, when multiple applications are launched, multiple Dalvik Virtual Machine instances occur that consume memory and time. To avoid that. Android Implements a process that enables low memory consumption and quick start-up time. What is the process called?

A. init
B. Media server
C. Zygote
D. Daemon

Answer: C

NEW QUESTION 247
- (Exam Topic 4)
Simona has written a regular expression for the detection of web application-specific attack attempt that reads as /((\%3C)|<K(\%2F)|V)*[a-zO-9\%I*((\%3E)|>)/Ix. Which of the following does the part (|\%3E)|>) look for?

A. Alphanumeric string or its hex equivalent
B. Opening angle bracket or its hex equivalent
C. Closing angle bracket or its hex equivalent
D. Forward slash for a closing tag or its hex equivalent

Answer: D

NEW QUESTION 251
- (Exam Topic 4)
A forensic examiner encounters a computer with a failed OS installation and the master boot record (MBR) or partition sector damaged. Which of the following tools can find and restore files and Information In the disk?

A. Helix
B. R-Studio
C. NetCat
D. Wireshark

Answer: B

NEW QUESTION 252

- (Exam Topic 4)
In a FIlesystem Hierarchy Standard (FHS), which of the following directories contains the binary files required for working?

A. /sbin
B. /proc
C. /mm
D. /media

Answer: A

NEW QUESTION 257
- (Exam Topic 4)
Jeff is a forensics investigator for a government agency's cyber security office. Jeff Is tasked with acquiring a memory dump of a Windows 10 computer that was involved In a DDoS attack on the government agency's web application. Jeff is onsite to collect the memory. What tool could Jeff use?

A. Volatility
B. Autopsy
C. RAM Mapper
D. Memcheck

Answer: A

NEW QUESTION 259
- (Exam Topic 4)
Which of the following statements pertaining to First Response is true?

A. First Response is a part of the investigation phase
B. First Response is a part of the post-investigation phase
C. First Response is a part of the pre-investigation phase
D. First Response is neither a part of pre-investigation phase nor a part of investigation phas
E. It only involves attending to a crime scene first and taking measures that assist forensic investigators in executing their tasks in the investigation phase more efficiently

Answer: A

NEW QUESTION 261
- (Exam Topic 4)
Rule 1002 of Federal Rules of Evidence (US) talks about

A. Admissibility of original
B. Admissibility of duplicates
C. Requirement of original
D. Admissibility of other evidence of contents

Answer: C

NEW QUESTION 265
- (Exam Topic 4)
You are an information security analyst at a large pharmaceutical company. While performing a routine review of audit logs, you have noticed a significant amount of egress traffic to various IP addresses on destination port 22 during off-peak hours. You researched some of the IP addresses and found that many of them are in Eastern Europe. What is the most likely cause of this traffic?

A. Malicious software on internal system is downloading research data from partner 5FTP servers in Eastern Europe
B. Internal systems are downloading automatic Windows updates
C. Data is being exfiltrated by an advanced persistent threat (APT)
D. The organization's primary internal DNS server has been compromised and is performing DNS zone transfers to malicious external entities

Answer: C

NEW QUESTION 267
- (Exam Topic 4)
The information security manager at a national legal firm has received several alerts from the intrusion detection system that a known attack signature was detected against the organization's file server. What should the information security manager do first?

A. Report the incident to senior management
B. Update the anti-virus definitions on the file server
C. Disconnect the file server from the network
D. Manually investigate to verify that an incident has occurred

Answer: C

NEW QUESTION 271
- (Exam Topic 4)
Maria has executed a suspicious executable file In a controlled environment and wants to see if the file adds/modifies any registry value after execution via Windows Event Viewer. Which of the following event ID should she look for In this scenario?

A. Event ID 4657

B. Event ID 4624
C. Event ID 4688
D. Event ID 7040

Answer: A

NEW QUESTION 273
- (Exam Topic 4)
Which of the following applications will allow a forensic investigator to track the user login sessions and user transactions that have occurred on an MS SQL Server?

A. ApexSQL Audit
B. netcat
C. Notepad++
D. Event Log Explorer

Answer: A

NEW QUESTION 277
- (Exam Topic 4)
Which of the following is the most effective tool for acquiring volatile data from a Windows-based system?

A. Coreography
B. Datagrab
C. Ethereal
D. Helix

Answer: D

NEW QUESTION 282
- (Exam Topic 4)
Fill In the missing Master Boot Record component.
* 1. Master boot code
* 2. Partition table
* 3. _____

A. Boot loader
B. Signature word
C. Volume boot record
D. Disk signature

Answer: A

NEW QUESTION 285
- (Exam Topic 4)
Which following forensic tool allows investigator to detect and extract hidden streams on NTFS drive?

A. Stream Detector
B. TimeStomp
C. Autopsy
D. analyzeMFT

Answer: A

NEW QUESTION 289
- (Exam Topic 4)
Frank, a cloud administrator in his company, needs to take backup of the OS disks of two Azure VMs that store business-critical data. Which type of Azure blob storage can he use for this purpose?

A. Append blob
B. Medium blob
C. Block blob
D. Page blob

Answer: D

NEW QUESTION 293
- (Exam Topic 4)
Sally accessed the computer system that holds trade secrets of the company where she Is employed. She knows she accessed It without authorization and all access (authorized and unauthorized) to this computer Is monitored.To cover her tracks. Sally deleted the log entries on this computer. What among the following best describes her action?

A. Password sniffing
B. Anti-forensics
C. Brute-force attack
D. Network intrusion

Answer: B

NEW QUESTION 296
- (Exam Topic 4)
Cloud forensic investigations impose challenges related to multi-jurisdiction and multi-tenancy aspects. To have a better understanding of the roles and responsibilities between the cloud service provider (CSP) and the client, which document should the forensic investigator review?

A. Service level agreement
B. Service level management
C. National and local regulation
D. Key performance indicator

Answer: A

NEW QUESTION 299
- (Exam Topic 4)
Donald made an OS disk snapshot of a compromised Azure VM under a resource group being used by the affected company as a part of forensic analysis process. He then created a vhd file out of the snapshot and stored it in a file share and as a page blob as backup in a storage account under different region. What Is the next thing he should do as a security measure?

A. Recommend changing the access policies followed by the company
B. Delete the snapshot from the source resource group
C. Delete the OS disk of the affected VM altogether
D. Create another VM by using the snapshot

Answer: C

NEW QUESTION 301
- (Exam Topic 4)
For the purpose of preserving the evidentiary chain of custody, which of the following labels is not appropriate?

A. Relevant circumstances surrounding the collection
B. General description of the evidence
C. Exact location the evidence was collected from
D. SSN of the person collecting the evidence

Answer: D

NEW QUESTION 306
- (Exam Topic 4)
SO/IEC 17025 is an accreditation for which of the following:

A. CHFI issuing agency
B. Encryption
C. Forensics lab licensing
D. Chain of custody

Answer: C

NEW QUESTION 311
- (Exam Topic 4)
An EC2 instance storing critical data of a company got infected with malware. The forensics team took the EBS volume snapshot of the affected Instance to perform further analysis and collected other data of evidentiary value. What should be their next step?

A. They should pause the running instance
B. They should keep the instance running as it stores critical data
C. They should terminate all instances connected via the same VPC
D. They should terminate the instance after taking necessary backup

Answer: D

NEW QUESTION 316
- (Exam Topic 4)
Recently, an Internal web app that a government agency utilizes has become unresponsive, Betty, a network engineer for the government agency, has been tasked to determine the cause of the web application's unresponsiveness. Betty launches Wlreshark and begins capturing the traffic on the local network. While analyzing the results, Betty noticed that a syn flood attack was underway. How did Betty know a syn flood attack was occurring?

A. Wireshark capture shows multiple ACK requests and SYN responses from single/multiple IP address(es)
B. Wireshark capture does not show anything unusual and the issue is related to the web application
C. Wireshark capture shows multiple SYN requests and RST responses from single/multiple IP address(es)
D. Wireshark capture shows multiple SYN requests and ACK responses from single/multiple IP address(es)

Answer: C

NEW QUESTION 317

- (Exam Topic 4)
Place the following In order of volatility from most volatile to the least volatile.

A. Registers and cache, routing tables, temporary file systems, disk storage, archival media
B. Register and cache, temporary file systems, routing tables, disk storage, archival media
C. Registers and cache, routing tables, temporary file systems, archival media, disk storage
D. Archival media, temporary file systems, disk storage, archival media, register and cache

Answer: B

NEW QUESTION 319
- (Exam Topic 4)
To understand the impact of a malicious program after the booting process and to collect recent information from the disk partition, an Investigator should evaluate the content of the:

A. MBR
B. GRUB
C. UEFI
D. BIOS

Answer: A

NEW QUESTION 320
- (Exam Topic 3)
Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?

A. Mime-Version header
B. Content-Type header
C. Content-Transfer-Encoding header
D. Errors-To header

Answer: D

NEW QUESTION 322
- (Exam Topic 4)
Data density of a disk drive is calculated by using

A. Slack space, bit density, and slack density.
B. Track space, bit area, and slack space.
C. Track density, areal density, and slack density.
D. Track density, areal density, and bit density.

Answer: D

NEW QUESTION 323
- (Exam Topic 3)
Which of the following standard represents a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?

A. SWGDE & SWGIT
B. Daubert
C. Frye
D. IOCE

Answer: C

NEW QUESTION 328
- (Exam Topic 3)
Which of the following Perl scripts will help an investigator to access the executable image of a process?

A. Lspd.pl
B. Lpsi.pl
C. Lspm.pl
D. Lspi.pl

Answer: D

NEW QUESTION 331
- (Exam Topic 3)
Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

A. FAT File System
B. ReFS
C. exFAT
D. NTFS File System

Answer: D

NEW QUESTION 332
- (Exam Topic 3)
The Recycle Bin exists as a metaphor for throwing files away, but it also allows a user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin. Which of the following files contains records that correspond to each deleted file in the Recycle Bin?

A. INFO2
B. INFO1
C. LOGINFO1
D. LOGINFO2

Answer: D

NEW QUESTION 337
- (Exam Topic 3)
Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the _____. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

A. Adjacent memory locations
B. Adjacent bit blocks
C. Adjacent buffer locations
D. Adjacent string locations

Answer: A

NEW QUESTION 341
- (Exam Topic 3)
What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?

A. Windows Services Monitoring
B. System Baselining
C. Start-up Programs Monitoring
D. Host integrity Monitoring

Answer: D

NEW QUESTION 343
- (Exam Topic 3)
Hard disk data addressing is a method of allotting addresses to each _____ of data on a hard disk.

A. Physical block
B. Operating system block
C. Hard disk block
D. Logical block

Answer: A

NEW QUESTION 346
- (Exam Topic 3)
During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

A. Rule 1003: Admissibility of Duplicates
B. Limited admissibility
C. Locard's Principle
D. Hearsay

Answer: B

NEW QUESTION 347
- (Exam Topic 3)
What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?

A. Jump instruction and the OEM ID
B. BIOS Parameter Block (BPB) and the OEM ID
C. BIOS Parameter Block (BPB) and the extended BPB
D. Bootstrap code and the end of the sector marker

Answer: C

NEW QUESTION 350
- (Exam Topic 3)
A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees don't like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

A. tcp.port = 23
B. tcp.port == 21
C. tcp.port == 21 || tcp.port == 22
D. tcp.port != 21

Answer: B

NEW QUESTION 351
- (Exam Topic 3)
Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

A. Model.log
B. Model.txt
C. Model.ldf
D. Model.lgf

Answer: C

NEW QUESTION 356
- (Exam Topic 3)
Which of the following commands shows you the username and IP address used to access the system via a remote login session and the type of client from which they are accessing the system?

A. Net config
B. Net sessions
C. Net share
D. Net stat

Answer: B

NEW QUESTION 357
- (Exam Topic 3)
Amber, a black hat hacker, has embedded malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

A. Malvertising
B. Compromising a legitimate site
C. Click-jacking
D. Spearphishing

Answer: A

NEW QUESTION 361
- (Exam Topic 3)
Which among the following U.S. laws requires financial institutions—companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance—to protect their customers' information against security threats?

A. SOX
B. HIPAA
C. GLBA
D. FISMA

Answer: C

NEW QUESTION 365
- (Exam Topic 3)
What document does the screenshot represent?

A. Expert witness form
B. Search warrant form
C. Chain of custody form
D. Evidence collection form

Answer: D

NEW QUESTION 367
- (Exam Topic 3)
Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

A. Server storage archives are the server information and settings stored on a local system, whereas the local archives are the local email client information stored on the mail server
B. It is difficult to deal with the webmail as there is no offline archive in most case
C. So consult your counsel on the case as to the best way to approach and gain access to the required data on servers
D. Local archives should be stored together with the server storage archives in order to be admissible in a court of law
E. Local archives do not have evidentiary value as the email client may alter the message data

Answer: B

NEW QUESTION 371
- (Exam Topic 3)
In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?

A. Cloud as an Object
B. Cloud as a Tool
C. Cloud as an Application
D. Cloud as a Subject

Answer: D

NEW QUESTION 372
- (Exam Topic 3)
What is the purpose of using Obfuscator in malware?

A. Execute malicious code in the system
B. Avoid encryption while passing through a VPN
C. Avoid detection by security mechanisms
D. Propagate malware to other connected devices

Answer: C

NEW QUESTION 374
- (Exam Topic 3)
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing . What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

A. Project Scope
B. Rules of Engagement
C. Non-Disclosure Agreement
D. Service Level Agreement

Answer: B

NEW QUESTION 378
- (Exam Topic 3)
Brian needs to acquire data from RAID storage. Which of the following acquisition methods is recommended to retrieve only the data relevant to the investigation?

A. Static Acquisition
B. Sparse or Logical Acquisition
C. Bit-stream disk-to-disk Acquisition
D. Bit-by-bit Acquisition

Answer: B

NEW QUESTION 380
- (Exam Topic 3)
Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?

A. ESE Database
B. Virtual Memory
C. Sparse files
D. Slack Space

Answer: A

NEW QUESTION 383
- (Exam Topic 3)
Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?

A. Dropper
B. Packer
C. Injector
D. Obfuscator

Answer: D

NEW QUESTION 385
- (Exam Topic 3)
In a Linux-based system, what does the command "Last -F" display?

A. Login and logout times and dates of the system
B. Last run processes
C. Last functions performed
D. Recently opened files

Answer: A

NEW QUESTION 386
- (Exam Topic 3)
Which type of attack is possible when attackers know some credible information about the victim's password, such as the password length, algorithms involved, or the strings and characters used in its creation?

A. Rule-Based Attack
B. Brute-Forcing Attack
C. Dictionary Attack
D. Hybrid Password Guessing Attack

Answer: A

NEW QUESTION 391
- (Exam Topic 3)
A forensic examiner is examining a Windows system seized from a crime scene. During the examination of a suspect file, he discovered that the file is password protected. He tried guessing the password using the suspect's available information but without any success. Which of the following tool can help the investigator to solve this issue?

A. Cain & Abel
B. Xplico
C. Recuva
D. Colasoft's Capsa

Answer: A

NEW QUESTION 395
- (Exam Topic 3)
Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.

A. DevScan
B. Devcon
C. fsutil
D. Reg.exe

Answer: B

NEW QUESTION 400
- (Exam Topic 3)
Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a
denial-of-service attack?

A. Email spamming
B. Phishing
C. Email spoofing
D. Mail bombing

Answer: D

NEW QUESTION 401
- (Exam Topic 3)
Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?

A. FISMA
B. HIPAA
C. GLBA
D. SOX

Answer: A

NEW QUESTION 404
- (Exam Topic 3)
What is the name of the first reserved sector in File allocation table?

A. Volume Boot Record
B. Partition Boot Sector
C. Master Boot Record
D. BIOS Parameter Block

Answer: C

NEW QUESTION 409
- (Exam Topic 3)
An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?

A. Name of the Database
B. Name of SQL Server
C. Operating system of the system
D. Network credentials of the database

Answer: B

NEW QUESTION 414
- (Exam Topic 3)
Gill is a computer forensics investigator who has been called upon to examine a seized computer. This computer, according to the police, was used by a hacker who gained access to numerous banking institutions to steal customer information. After preliminary investigations, Gill finds in the computer's log files that the hacker was able to gain access to these banks through the use of Trojan horses. The hacker then used these Trojan horses to obtain remote access to the companies' domain controllers. From this point, Gill found that the hacker pulled off the SAM files from the domain controllers to then attempt and crack network passwords. What is the most likely password cracking technique used by this hacker to break the user passwords from the SAM files?

A. Syllable attack
B. Hybrid attack
C. Brute force attack
D. Dictionary attack

Answer: D

NEW QUESTION 418
- (Exam Topic 3)
Which command can provide the investigators with details of all the loaded modules on a Linux-based system?

A. list modules -a
B. lsmod
C. plist mod -a
D. lsof -m

Answer: B

NEW QUESTION 423
- (Exam Topic 3)
Which U.S. law sets the rules for sending emails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of emails the right to ask the senders to stop emailing them, and spells out the penalties in case the above said rules are violated?

A. NO-SPAM Act
B. American: NAVSO P-5239-26 (RLL)
C. CAN-SPAM Act
D. American: DoD 5220.22-M

Answer: C

NEW QUESTION 428
- (Exam Topic 3)
Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?

A. Cross Examination
B. Direct Examination
C. Indirect Examination
D. Witness Examination

Answer: A

NEW QUESTION 433
- (Exam Topic 3)
Select the tool appropriate for examining the dynamically linked libraries of an application or malware.

A. DependencyWalker
B. SysAnalyzer
C. PEiD
D. ResourcesExtract

Answer: A

NEW QUESTION 434
- (Exam Topic 3)
POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?

A. 110
B. 143
C. 25
D. 993

Answer: A

NEW QUESTION 439
- (Exam Topic 3)
Consider that you are investigating a machine running an Windows OS released prior to Windows Vista. You are trying to gather information about the deleted files by examining the master database file named INFO2 located at C:\Recycler\<USER SID>\. You read an entry named "Dd5.exe". What does Dd5.exe mean?

A. D driv
B. fifth file deleted, a .exe file
C. D drive, fourth file restored, a .exe file
D. D drive, fourth file deleted, a .exe file
E. D drive, sixth file deleted, a .exe file

Answer: B

NEW QUESTION 444
- (Exam Topic 3)
Which of the following components within the android architecture stack take care of displaying windows owned by different applications?

A. Media Framework
B. Surface Manager
C. Resource Manager
D. Application Framework

Answer: D

NEW QUESTION 447
- (Exam Topic 3)
Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

A. HKEY_CLASSES_ROOT
B. HKEY_CURRENT_CONFIG
C. HKEY_LOCAL_MACHINE
D. HKEY_USERS

Answer: A

NEW QUESTION 452
- (Exam Topic 3)
When a user deletes a file, the system creates a $I file to store its details. What detail does the $I file not contain?

A. File Size
B. File origin and modification
C. Time and date of deletion
D. File Name

Answer: B

NEW QUESTION 456
- (Exam Topic 3)
Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?

A. pstree

B. pgrep
C. ps
D. grep

Answer: B

NEW QUESTION 460
- (Exam Topic 3)
What is the location of a Protective MBR in a GPT disk layout?

A. Logical Block Address (LBA) 2
B. Logical Block Address (LBA) 0
C. Logical Block Address (LBA) 1
D. Logical Block Address (LBA) 3

Answer: C

NEW QUESTION 462
- (Exam Topic 3)
Which of the following protocols allows non-ASCII files, such as video, graphics, and audio, to be sent through the email messages?

A. MIME
B. BINHEX
C. UT-16
D. UUCODE

Answer: A

NEW QUESTION 464
- (Exam Topic 3)
What is the framework used for application development for iOS-based mobile devices?

A. Cocoa Touch
B. Dalvik
C. Zygote
D. AirPlay

Answer: A

NEW QUESTION 467
- (Exam Topic 3)
Which of the following statements is true regarding SMTP Server?

A. SMTP Server breaks the recipient's address into Recipient's name and his/her designation before passing it to the DNS Server
B. SMTP Server breaks the recipient's address into Recipient's name and recipient's address before passing it to the DNS Server
C. SMTP Server breaks the recipient's address into Recipient's name and domain name before passing it to the DNS Server
D. SMTP Server breaks the recipient's address into Recipient's name and his/her initial before passing it to the DNS Server

Answer: C

NEW QUESTION 472
- (Exam Topic 3)
James is dealing with a case regarding a cybercrime that has taken place in Arizona, USA. James needs to lawfully seize the evidence from an electronic device without affecting the user's anonymity. Which of the following law should he comply with, before retrieving the evidence?

A. First Amendment of the U.
B. Constitution
C. Fourth Amendment of the U.
D. Constitution
E. Third Amendment of the U.
F. Constitution
G. Fifth Amendment of the U.
H. Constitution

Answer: D

NEW QUESTION 476
- (Exam Topic 3)
You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a "simple backup copy" of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a "simple backup copy" will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

A. Robust copy
B. Incremental backup copy
C. Bit-stream copy

D. Full backup copy

Answer: C

NEW QUESTION 480
- (Exam Topic 3)
Robert, a cloud architect, received a huge bill from the cloud service provider, which usually doesn't happen. After analyzing the bill, he found that the cloud resource consumption was very high. He then examined the cloud server and discovered that a malicious code was running on the server, which was generating huge but harmless traffic from the server. This means that the server has been compromised by an attacker with the sole intention to hurt the cloud customer financially. Which attack is described in the above scenario?

A. XSS Attack
B. DDoS Attack (Distributed Denial of Service)
C. Man-in-the-cloud Attack
D. EDoS Attack (Economic Denial of Service)

Answer: B

NEW QUESTION 484
- (Exam Topic 3)
Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?

A. Remote File Inclusion
B. Cross Site Scripting
C. Insecure Direct Object References
D. Cross Site Request Forgery

Answer: C

NEW QUESTION 485
- (Exam Topic 3)
What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?
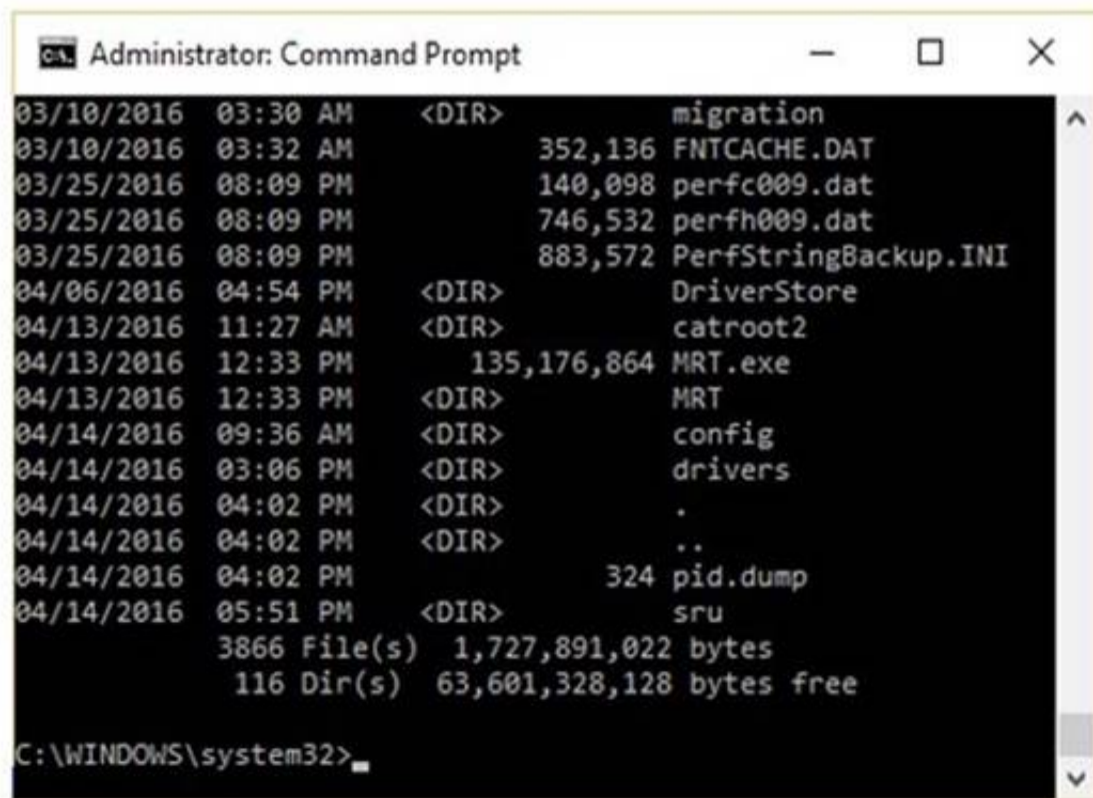
A. AA55
B. 00AA
C. AA00
D. A100

Answer: A

NEW QUESTION 486
- (Exam Topic 3)
The given image displays information about date and time of installation of the OS along with service packs, patches, and sub-directories. What command or tool did the investigator use to view this output?

A. dir /o:d
B. dir /o:s
C. dir /o:e
D. dir /o:n

Answer: A

NEW QUESTION 488
- (Exam Topic 3)
In which of these attacks will a steganalyst use a random message to generate a stego-object by using some steganography tool, to find the steganography algorithm used to hide the information?

A. Chosen-message attack
B. Known-cover attack
C. Known-message attack
D. Known-stego attack

Answer: A

NEW QUESTION 491
- (Exam Topic 3)
When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

A. UTC
B. PTP
C. Time Protocol
D. NTP

Answer: D

NEW QUESTION 492
- (Exam Topic 3)
Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?

A. Same-platform correlation
B. Network-platform correlation
C. Cross-platform correlation
D. Multiple-platform correlation

Answer: C

NEW QUESTION 497
- (Exam Topic 3)
What does the Rule 101 of Federal Rules of Evidence states?

A. Scope of the Rules, where they can be applied
B. Purpose of the Rules
C. Limited Admissibility of the Evidence
D. Rulings on Evidence

Answer: A

NEW QUESTION 502
- (Exam Topic 3)
Which component in the hard disk moves over the platter to read and write information?

A. Actuator
B. Spindle
C. Actuator Axis
D. Head

Answer: D

NEW QUESTION 505
- (Exam Topic 3)
Which Linux command when executed displays kernel ring buffers or information about device drivers loaded into the kernel?

A. pgrep
B. dmesg
C. fsck
D. grep

Answer: B

NEW QUESTION 508
- (Exam Topic 3)
What does Locard's Exchange Principle state?

A. Any information of probative value that is either stored or transmitted in a digital form
B. Digital evidence must have some characteristics to be disclosed in the court of law
C. Anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave
D. Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence

Answer: C

NEW QUESTION 509
- (Exam Topic 3)
Report writing is a crucial stage in the outcome of an investigation. Which information should not be included in the report section?

A. Speculation or opinion as to the cause of the incident
B. Purpose of the report
C. Author of the report
D. Incident summary

Answer: A

NEW QUESTION 510
- (Exam Topic 3)
Jim's company regularly performs backups of their critical servers. But the company can't afford to send backup tapes to an off-site vendor for long term storage and archiving. Instead Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes aren't stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?

A. Encrypt the backup tapes and use a courier to transport them.
B. Encrypt the backup tapes and transport them in a lock box
C. Degauss the backup tapes and transport them in a lock box.
D. Hash the backup tapes and transport them in a lock box.

Answer: B

NEW QUESTION 513
- (Exam Topic 3)
Which of the following is a device monitoring tool?

A. Capsa
B. Driver Detective
C. Regshot
D. RAM Capturer

Answer: A

NEW QUESTION 514
- (Exam Topic 3)
Which of the following tools is not a data acquisition hardware tool?

A. UltraKit
B. Atola Insight Forensic
C. F-Response Imager
D. Triage-Responder

Answer: C

NEW QUESTION 517
- (Exam Topic 3)
Which of the following is a responsibility of the first responder?

A. Determine the severity of the incident
B. Collect as much information about the incident as possible
C. Share the collected information to determine the root cause
D. Document the findings

Answer: B

NEW QUESTION 519
- (Exam Topic 3)
Lynne receives the following email:
Dear lynne@gmail.com! We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11/10 20:40:24
You have 24 hours to fix this problem or risk to be closed permanently! To proceed Please Connect >> My Apple ID
Thank You The link to My Apple ID shows http://byggarbetsplatsen.se/backup/signon/ What type of attack is this?

A. Mail Bombing
B. Phishing
C. Email Spamming
D. Email Spoofing

Answer: B

NEW QUESTION 523

- (Exam Topic 3)
What does the command "C:\>wevtutil gl <log name>" display?

A. Configuration information of a specific Event Log
B. Event logs are saved in .xml format
C. Event log record structure
D. List of available Event Logs

Answer: A

NEW QUESTION 528
- (Exam Topic 3)
Which of the following techniques delete the files permanently?

A. Steganography
B. Artifact Wiping
C. Data Hiding
D. Trail obfuscation

Answer: B

NEW QUESTION 533
- (Exam Topic 3)
As a part of the investigation, Caroline, a forensic expert, was assigned the task to examine the transaction logs pertaining to a database named Transfers. She used SQL Server Management Studio to collect the active transaction log files of the database. Caroline wants to extract detailed information on the logs, including AllocUnitId, page id, slot id, etc. Which of the following commands does she need to execute in order to extract the desired information?

A. DBCC LOG(Transfers, 1)
B. DBCC LOG(Transfers, 3)
C. DBCC LOG(Transfers, 0)
D. DBCC LOG(Transfers, 2)

Answer: D

NEW QUESTION 537
- (Exam Topic 3)
Which of the following files contains the traces of the applications installed, run, or uninstalled from a system?

A. Virtual Files
B. Image Files
C. Shortcut Files
D. Prefetch Files

Answer: C

NEW QUESTION 540
- (Exam Topic 3)
Which of the following statements is TRUE about SQL Server error logs?

A. SQL Server error logs record all the events occurred on the SQL Server and its databases
B. Forensic investigator uses SQL Server Profiler to view error log files
C. Error logs contain IP address of SQL Server client connections
D. Trace files record, user-defined events, and specific system events

Answer: B

NEW QUESTION 543
- (Exam Topic 3)
Which of the following is a part of a Solid-State Drive (SSD)?

A. Head
B. Cylinder
C. NAND-based flash memory
D. Spindle

Answer: C

NEW QUESTION 547
- (Exam Topic 3)
In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

A. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
B. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
C. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name
D. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
E. In a pharming attack an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name

F. Both pharming and phishing attacks are identical

Answer: B

NEW QUESTION 552
- (Exam Topic 3)
Examination of a computer by a technically unauthorized person will almost always result in:

A. Rendering any evidence found inadmissible in a court of law
B. Completely accurate results of the examination
C. The chain of custody being fully maintained
D. Rendering any evidence found admissible in a court of law

Answer: A

NEW QUESTION 553
- (Exam Topic 3)
Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot records, or memory with a known and trusted baseline?

A. Signature-Based Detection
B. Integrity-Based Detection
C. Cross View-Based Detection
D. Heuristic/Behavior-Based Detection

Answer: B

NEW QUESTION 555
- (Exam Topic 3)
UEFI is a specification that defines a software interface between an OS and platform firmware. Where does this interface store information about files present on a disk?

A. BIOS-MBR
B. GUID Partition Table (GPT)
C. Master Boot Record (MBR)
D. BIOS Parameter Block

Answer: B

NEW QUESTION 556
- (Exam Topic 3)
Identify the term that refers to individuals who, by virtue of their knowledge and expertise, express an independent opinion on a matter related to a case based on the information that is provided.

A. Expert Witness
B. Evidence Examiner
C. Forensic Examiner
D. Defense Witness

Answer: A

NEW QUESTION 560
- (Exam Topic 3)
In Windows, prefetching is done to improve system performance. There are two types of prefetching: boot prefetching and application prefetching. During boot prefetching, what does the Cache Manager do?

A. Determines the data associated with value EnablePrefetcher
B. Monitors the first 10 seconds after the process is started
C. Checks whether the data is processed
D. Checks hard page faults and soft page faults

Answer: C

NEW QUESTION 562
- (Exam Topic 3)
Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?

A. A text file deleted from C drive in sixth sequential order
B. A text file deleted from C drive in fifth sequential order
C. A text file copied from D drive to C drive in fifth sequential order
D. A text file copied from C drive to D drive in fifth sequential order

Answer: B

NEW QUESTION 563

- (Exam Topic 3)
An attacker successfully gained access to a remote Windows system and plans to install persistent backdoors on it. Before that, to avoid getting detected in future, he wants to cover his tracks by disabling the
last-accessed timestamps of the machine. What would he do to achieve this?

A. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 0
B. Run the command fsutil behavior set disablelastaccess 0
C. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 1
D. Run the command fsutil behavior set enablelastaccess 0

Answer: C

NEW QUESTION 568
- (Exam Topic 2)
What is one method of bypassing a system BIOS password?

A. Removing the processor
B. Removing the CMOS battery
C. Remove all the system memory
D. Login to Windows and disable the BIOS password

Answer: B

NEW QUESTION 573
- (Exam Topic 2)
Where is the startup configuration located on a router?

A. Static RAM
B. BootROM
C. NVRAM
D. Dynamic RAM

Answer: C

NEW QUESTION 577
- (Exam Topic 2)
Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a $Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

A. Windows 98
B. Linux
C. Windows 8.1
D. Windows XP

Answer: D

NEW QUESTION 581
- (Exam Topic 2)
To which phase of the Computer Forensics Investigation Process does the Planning and Budgeting of a Forensics Lab belong?

A. Post-investigation Phase
B. Reporting Phase
C. Pre-investigation Phase
D. Investigation Phase

Answer: C

NEW QUESTION 586
- (Exam Topic 2)
In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers Version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
        Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
        by smtp1.somedomain.com (8.13.1/8.12.11) with ESMTP id l51EfCEh032241
        for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
        Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange V6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewherelese.com>
MIME-Version: 1.0
```

A. Somedomain.com
B. Smtp1.somedomain.com
C. Simon1.state.ok.gov.us

D. David1.state.ok.gov.us

Answer: C

NEW QUESTION 591
- (Exam Topic 2)
What type of analysis helps to identify the time and sequence of events in an investigation?
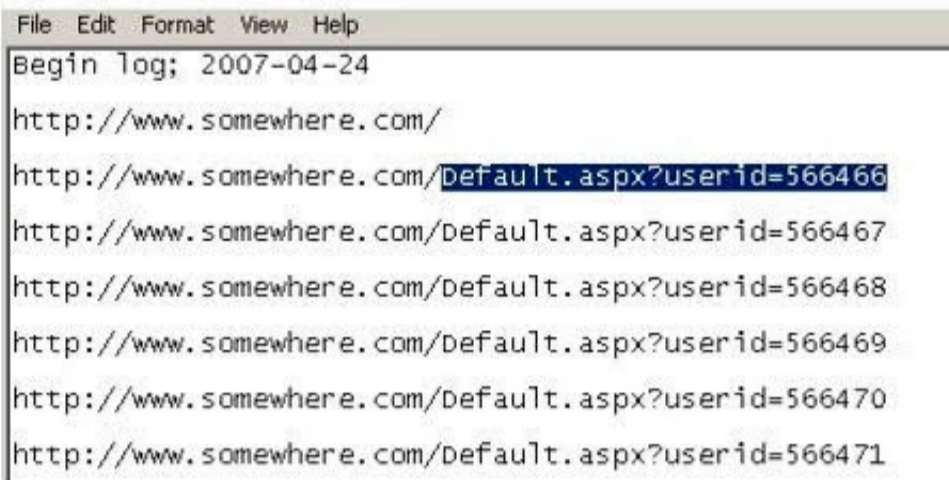
A. Time-based
B. Functional
C. Relational
D. Temporal

Answer: D

NEW QUESTION 592
- (Exam Topic 2)
Using Internet logging software to investigate a case of malicious use of computers, the investigator comes across some entries that appear odd.


```
File Edit Format View Help
Begin log; 2007-04-24
http://www.somewhere.com/
http://www.somewhere.com/Default.aspx?userid=566466
http://www.somewhere.com/Default.aspx?userid=566467
http://www.somewhere.com/Default.aspx?userid=566468
http://www.somewhere.com/Default.aspx?userid=566469
http://www.somewhere.com/Default.aspx?userid=566470
http://www.somewhere.com/Default.aspx?userid=566471
```

From the log, the investigator can see where the person in question went on the Internet. From the log, it appears that the user was manually typing in different user ID numbers. What technique this user was trying?

A. Parameter tampering
B. Cross site scripting
C. SQL injection
D. Cookie Poisoning

Answer: A

NEW QUESTION 593
- (Exam Topic 2)
Netstat is a tool for collecting information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

A. netstat – r
B. netstat – ano
C. netstat – b
D. netstat – s

Answer: B

NEW QUESTION 598
- (Exam Topic 2)
Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?

A. filecache.db
B. config.db
C. sigstore.db
D. Sync_config.db

Answer: D

NEW QUESTION 600
- (Exam Topic 2)
Which of the following Event Correlation Approach is an advanced correlation method that assumes and predicts what an attacker can do next after the attack by studying the statistics and probability and uses only two variables?

A. Bayesian Correlation
B. Vulnerability-Based Approach
C. Rule-Based Approach
D. Route Correlation

Answer: A

NEW QUESTION 601
- (Exam Topic 2)
Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company PBX system be called?

A. Phreaking
B. Squatting
C. Crunching
D. Pretexting

Answer: A

NEW QUESTION 605
- (Exam Topic 2)
Which program is the bootloader when Windows XP starts up?

A. KERNEL.EXE
B. NTLDR
C. LOADER
D. LILO

Answer: B

NEW QUESTION 608
- (Exam Topic 2)
Where is the default location for Apache access logs on a Linux computer?

A. usr/local/apache/logs/access_log
B. bin/local/home/apache/logs/access_log
C. usr/logs/access_log
D. logs/usr/apache/access_log

Answer: A

NEW QUESTION 609
- (Exam Topic 2)

A. 202
B. 404
C. 606
D. 999

Answer: B

NEW QUESTION 611
- (Exam Topic 2)
Which of the following is NOT a part of pre-investigation phase?

A. Building forensics workstation
B. Gathering information about the incident
C. Gathering evidence data
D. Creating an investigation team

Answer: C

NEW QUESTION 612
- (Exam Topic 2)
In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A. The change in the routing fabric to bypass the affected router
B. More RESET packets to the affected router to get it to power back up
C. RESTART packets to the affected router to get it to power back up
D. STOP packets to all other routers warning of where the attack originated

Answer: A

NEW QUESTION 617
- (Exam Topic 2)
You have been called in to help with an investigation of an alleged network intrusion. After questioning the members of the company IT department, you search through the server log files to find any trace of the intrusion. After that you decide to telnet into one of the company routers to see if there is any evidence to be found. While connected to the router, you see some unusual activity and believe that the attackers are currently connected to that router. You start up an ethereal session to begin capturing traffic on the router that could be used in the investigation. At what layer of the OSI model are you monitoring while watching traffic to

and from the router?

A. Network
B. Transport
C. Data Link
D. Session

Answer: A

NEW QUESTION 621
- (Exam Topic 2)
Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?

A. IT personnel
B. Employees themselves
C. Supervisors
D. Administrative assistant in charge of writing policies

Answer: C

NEW QUESTION 625
- (Exam Topic 2)
A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?

A. He should search in C:\Windows\System32\RECYCLED folder
B. The Recycle Bin does not exist on the hard drive
C. The files are hidden and he must use switch to view them
D. Only FAT system contains RECYCLED folder and not NTFS

Answer: C

NEW QUESTION 626
- (Exam Topic 2)
A computer forensics investigator is inspecting the firewall logs for a large financial institution that has employees working 24 hours a day, 7 days a week.

What can the investigator infer from the screenshot seen below?

A. A smurf attack has been attempted
B. A denial of service has been attempted
C. Network intrusion has occurred
D. Buffer overflow attempt on the firewall.

Answer: C

NEW QUESTION 631
- (Exam Topic 2)
When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?

A. FF D8 FF E0 00 10
B. FF FF FF FF FF FF
C. FF 00 FF 00 FF 00
D. EF 00 EF 00 EF 00

Answer: A

NEW QUESTION 633
- (Exam Topic 2)
What will the following command accomplish in Linux? fdisk /dev/hda

A. Partition the hard drive
B. Format the hard drive
C. Delete all files under the /dev/hda folder
D. Fill the disk with zeros

Answer: A

NEW QUESTION 638
- (Exam Topic 2)
What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?

A. Repairs logical file system errors
B. Check the disk for hardware errors
C. Check the disk for connectivity errors
D. Check the disk for Slack Space

Answer: A

NEW QUESTION 641
- (Exam Topic 2)
Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

A. Record the system state by taking photographs of physical system and the display
B. Perform data acquisition without disturbing the state of the systems
C. Open the systems, remove the hard disk and secure it
D. Switch off the systems and carry them to the laboratory

Answer: A

NEW QUESTION 646
- (Exam Topic 2)
Which of the following tool enables a user to reset his/her lost admin password in a Windows system?

A. Advanced Office Password Recovery
B. Active@ Password Changer
C. Smartkey Password Recovery Bundle Standard
D. Passware Kit Forensic

Answer: B

NEW QUESTION 650
- (Exam Topic 2)
Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?

A. Written Formal Report
B. Verbal Formal Report
C. Verbal Informal Report
D. Written Informal Report

Answer: B

NEW QUESTION 651
- (Exam Topic 2)
Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

A. HIPAA
B. GLBA
C. SOX
D. FISMA

Answer: C

NEW QUESTION 654
- (Exam Topic 2)
The process of restarting a computer that is already turned on through the operating system is called?

A. Warm boot
B. Ice boot
C. Hot Boot
D. Cold boot

Answer: A

NEW QUESTION 658
- (Exam Topic 2)
Why would you need to find out the gateway of a device when investigating a wireless attack?

A. The gateway will be the IP of the proxy server used by the attacker to launch the attack
B. The gateway will be the IP of the attacker computer
C. The gateway will be the IP used to manage the RADIUS server
D. The gateway will be the IP used to manage the access point

Answer: D

NEW QUESTION 660
- (Exam Topic 2)
When needing to search for a website that is no longer present on the Internet today but was online few years back, what site can be used to view the website collection of pages?

A. Proxify.net
B. Dnsstuff.com
C. Samspade.org
D. Archive.org

Answer: D

NEW QUESTION 665
- (Exam Topic 2)
Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Block all internal MAC address from using SNMP
B. Block access to UDP port 171
C. Block access to TCP port 171
D. Change the default community string names

Answer: D

NEW QUESTION 667
- (Exam Topic 2)
Which US law does the interstate or international transportation and receiving of child pornography fall under?
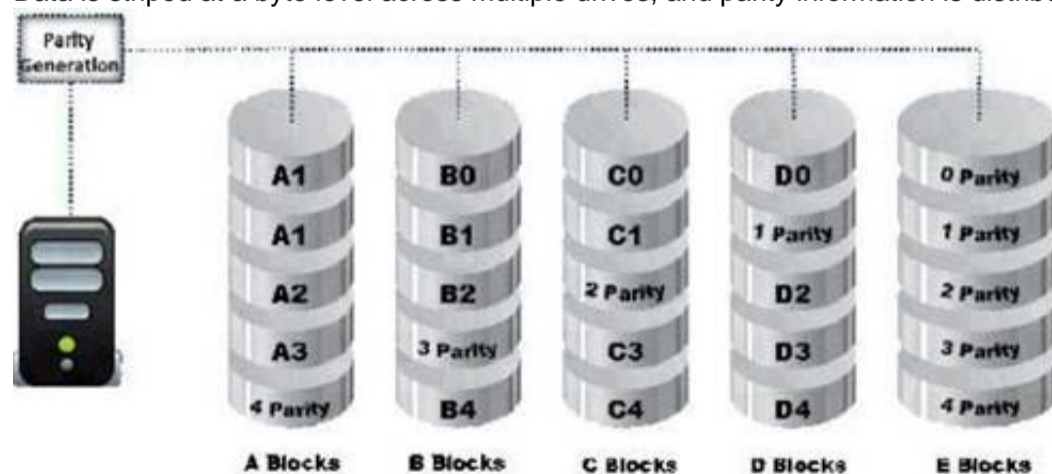
A. §18. U.S.
B. 1466A
C. §18. U.S.C 252
D. §18. U.S.C 146A
E. §18. U.S.C 2252

Answer: D

NEW QUESTION 668
- (Exam Topic 2)
Data is striped at a byte level across multiple drives, and parity information is distributed among all member drives.

What RAID level is represented here?

A. RAID Level 0
B. RAID Level 5
C. RAID Level 3
D. RAID Level 1

Answer: B

NEW QUESTION 671

- (Exam Topic 2)
What hashing method is used to password protect Blackberry devices?

A. AES
B. RC5
C. MD5
D. SHA-1

Answer: D

NEW QUESTION 675
- (Exam Topic 2)
Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS?

A. wmic service
B. Reg.exe
C. fsutil
D. Devcon

Answer: C

NEW QUESTION 679
- (Exam Topic 2)
An expert witness is a who is normally appointed by a party to assist the formulation and preparation of a party's claim or defense.

A. Expert in criminal investigation
B. Subject matter specialist
C. Witness present at the crime scene
D. Expert law graduate appointed by attorney

Answer: B

NEW QUESTION 681
- (Exam Topic 2)
What does the 63.78.199.4(161) denotes in a Cisco router log?
Mar 14 22:57:53.425 EST: %SEC-6-IPACCESSLOGP: list internet-inbound denied udp 66.56.16.77(1029) -> 63.78.199.4(161), 1 packet

A. Destination IP address
B. Source IP address
C. Login IP address
D. None of the above

Answer: A

NEW QUESTION 685
- (Exam Topic 2)
Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?

A. Sectors
B. Interface
C. Cylinder
D. Heads

Answer: B

NEW QUESTION 689
- (Exam Topic 2)
Which of the following refers to the process of the witness being questioned by the attorney who called the latter to the stand?

A. Witness Authentication
B. Direct Examination
C. Expert Witness
D. Cross Questioning

Answer: B

NEW QUESTION 692
- (Exam Topic 2)
Who is responsible for the following tasks?

A. Non-forensics staff
B. Lawyers
C. System administrators
D. Local managers or other non-forensic staff

Answer: A

NEW QUESTION 696
- (Exam Topic 2)
What layer of the OSI model do TCP and UDP utilize?

A. Data Link
B. Network
C. Transport
D. Session

Answer: C

NEW QUESTION 697
- (Exam Topic 2)
Which among the following search warrants allows the first responder to get the victim's computer information such as service records, billing records, and subscriber information from the service provider?

A. Citizen Informant Search Warrant
B. Electronic Storage Device Search Warrant
C. John Doe Search Warrant
D. Service Provider Search Warrant

Answer: B

NEW QUESTION 700
- (Exam Topic 2)
When a user deletes a file or folder, the system stores complete path including the original filename is a special hidden file called "INFO2" in the Recycled folder. If the INFO2 file is deleted, it is recovered when you .

A. Undo the last action performed on the system
B. Reboot Windows
C. Use a recovery tool to undelete the file
D. Download the file from Microsoft website

Answer: A

NEW QUESTION 701
- (Exam Topic 2)
When is it appropriate to use computer forensics?

A. If copyright and intellectual property theft/misuse has occurred
B. If employees do not care for their boss management techniques
C. If sales drop off for no apparent reason for an extended period of time
D. If a financial institution is burglarized by robbers

Answer: A

NEW QUESTION 702
- (Exam Topic 2)
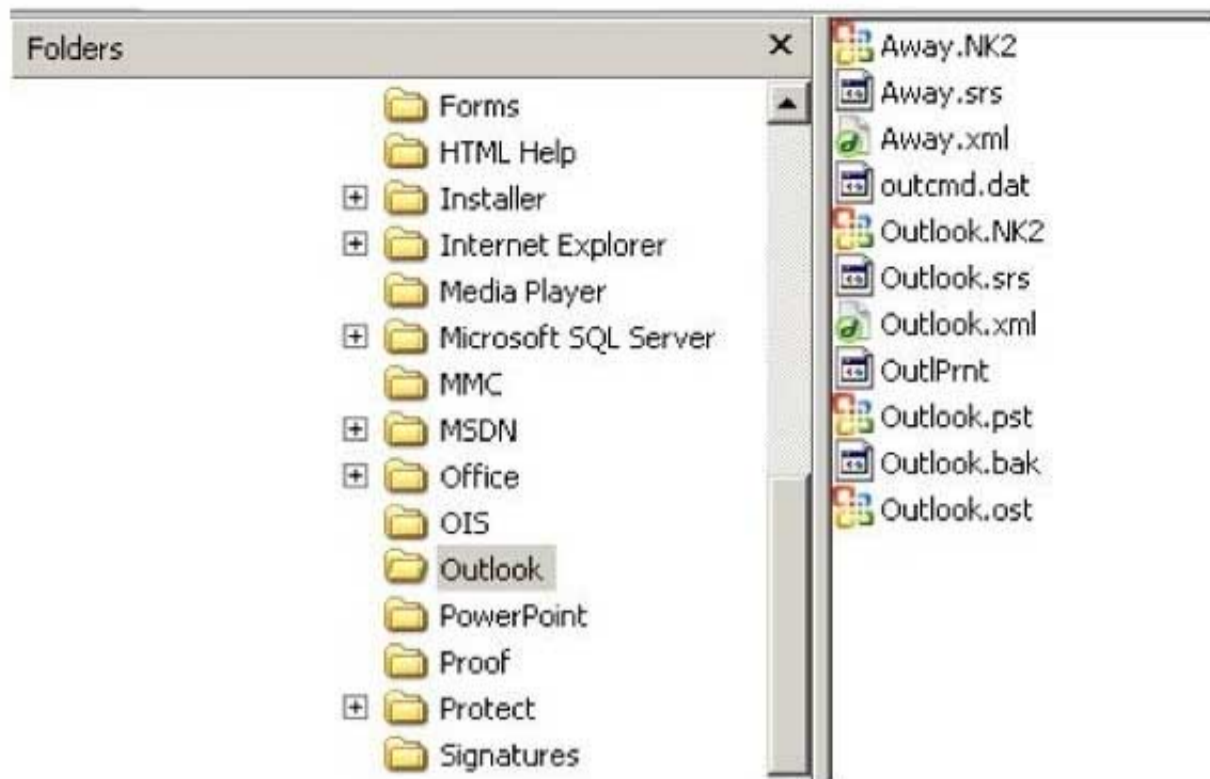Which among the following files provides email header information in the Microsoft Exchange server?

A. gwcheck.db
B. PRIV.EDB
C. PUB.EDB
D. PRIV.STM

Answer: B

NEW QUESTION 706
- (Exam Topic 2)
In the following directory listing,

Which file should be used to restore archived email messages for someone using Microsoft Outlook?

A. Outlook bak
B. Outlook ost
C. Outlook NK2
D. Outlook pst

Answer: D

NEW QUESTION 707
- (Exam Topic 2)
Which of the following tool enables data acquisition and duplication?

A. Colasoft's Capsa
B. DriveSpy
C. Wireshark
D. Xplico

Answer: B

NEW QUESTION 711
- (Exam Topic 2)
What type of flash memory card comes in either Type I or Type II and consumes only five percent of the power required by small hard drives?

A. SD memory
B. CF memory
C. MMC memory
D. SM memory

Answer: B

NEW QUESTION 712
- (Exam Topic 2)
What is the slave device connected to the secondary IDE controller on a Linux OS referred to?

A. hda
B. hdd
C. hdb
D. hdc

Answer: B

NEW QUESTION 717
- (Exam Topic 2)
Where does Encase search to recover NTFS files and folders?

A. MBR
B. MFT
C. Slack space
D. HAL

Answer: B

NEW QUESTION 722

- (Exam Topic 2)
Which of the following files DOES NOT use Object Linking and Embedding (OLE) technology to embed and link to other objects?

A. Portable Document Format
B. MS-office Word Document
C. MS-office Word OneNote
D. MS-office Word PowerPoint

Answer: A

NEW QUESTION 725
- (Exam Topic 2)
Wireless access control attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allow the attacker to set up a rogue access point outside the corporate perimeter and then lure the employees of the organization to connect to it?

A. Ad hoc associations
B. Client mis-association
C. MAC spoofing
D. Rogue access points

Answer: B

NEW QUESTION 730
- (Exam Topic 2)
Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?

A. Volume Boot Record
B. Master Boot Record
C. GUID Partition Table
D. Master File Table

Answer: D

NEW QUESTION 731
- (Exam Topic 2)
What is the default IIS log location?

A. SystemDrive\inetpub\LogFiles
B. %SystemDrive%\inetpub\logs\LogFiles
C. %SystemDrive\logs\LogFiles
D. SystemDrive\logs\LogFiles

Answer: B

NEW QUESTION 733
- (Exam Topic 2)
What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

A. Fraggle
B. Smurf scan
C. SYN flood
D. Teardrop

Answer: A

NEW QUESTION 735
- (Exam Topic 2)
Which code does the FAT file system use to mark the file as deleted?

A. ESH
B. 5EH
C. H5E
D. E5H

Answer: D

NEW QUESTION 737
- (Exam Topic 2)
Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the
PCs found in the hackers hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?

A. Place PDA, including all devices, in an antistatic bag
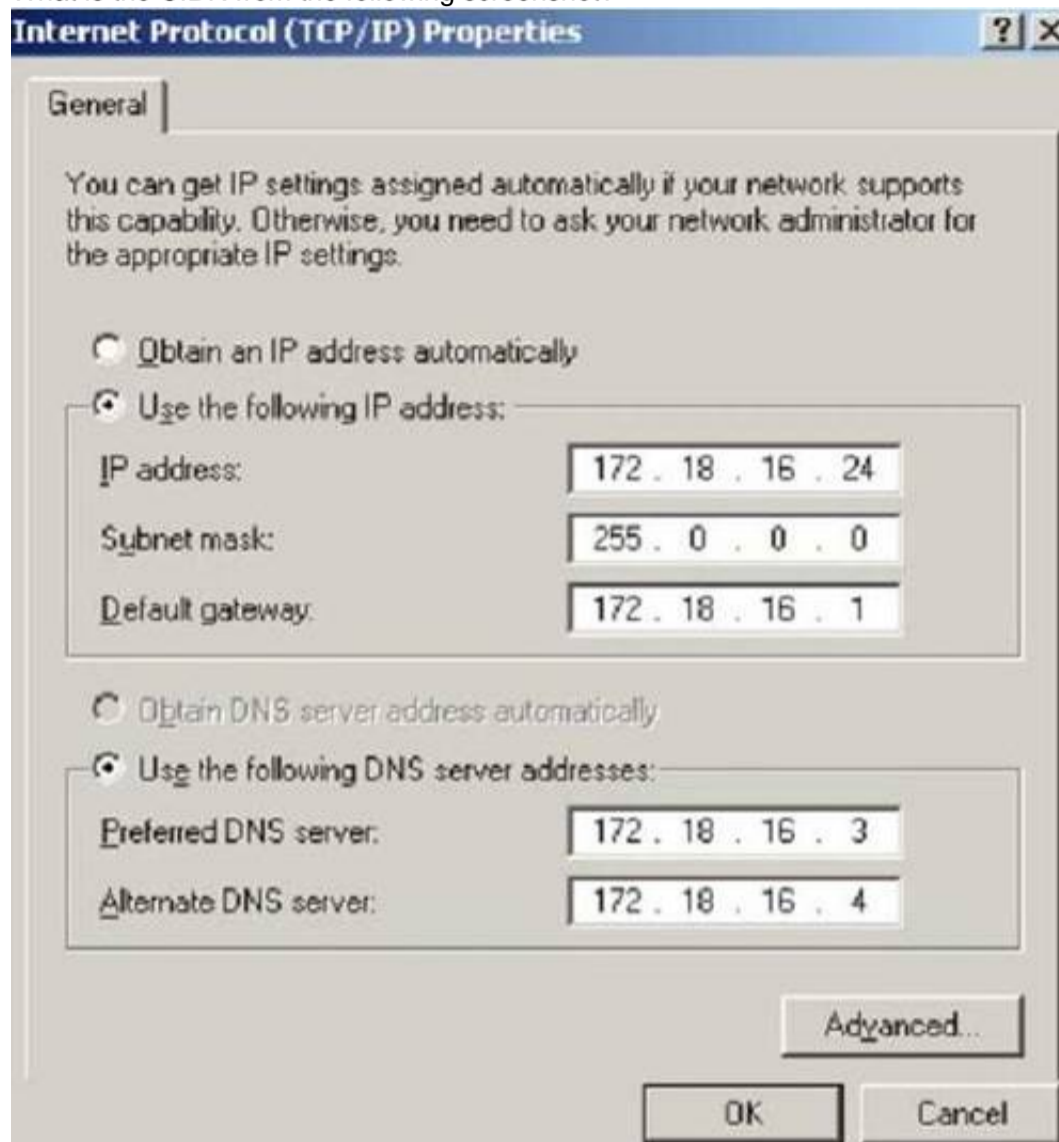B. Unplug all connected devices
C. Power off all devices if currently on

D. Photograph and document the peripheral devices

Answer: D

NEW QUESTION 741
- (Exam Topic 2)
What is the CIDR from the following screenshot?

A. /24A./24A./24
B. /32 B./32 B./32
C. /16 C./16 C./16
D. /8D./8D./8

Answer: D

NEW QUESTION 746
- (Exam Topic 2)
Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully. Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices. How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?

A. Two
B. One
C. Three
D. Four

Answer: A

NEW QUESTION 749
- (Exam Topic 2)
Which of the following tool captures and allows you to interactively browse the traffic on a network?

A. Security Task Manager
B. Wireshark
C. ThumbsDisplay
D. RegScanner

Answer: B

NEW QUESTION 751
- (Exam Topic 2)
Which MySQL log file contains information on server start and stop?

A. Slow query log file
B. General query log file
C. Binary log
D. Error log file

Answer: D

NEW QUESTION 753
- (Exam Topic 2)
What must be obtained before an investigation is carried out at a location?

A. Search warrant
B. Subpoena
C. Habeas corpus
D. Modus operandi

Answer: A

NEW QUESTION 755
- (Exam Topic 2)
While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?

A. Technical material related to forensics
B. No particular field
C. Judging the character of defendants/victims
D. Legal issues

Answer: B

NEW QUESTION 760
- (Exam Topic 2)
What is the location of the binary files required for the functioning of the OS in a Linux system?

A. /run
B. /bin
C. /root
D. /sbin

Answer: B

NEW QUESTION 765
- (Exam Topic 2)
The following is a log file screenshot from a default installation of IIS 6.0.

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2007-01-22 15:42:36
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-user
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /index.html - 80 - 172.16.28.80
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/index.asp - 80 - 172.16.28
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/css/olcStyle.css - 80 - 17
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /favicon.ico - 80 - 172.16.28.80 Avant+
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/css/dhtml_horiz.css - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_03.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_04.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_06.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_07.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_08.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/script/dhtml.js - 80 - 172
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/greenArraw.jpg - 80
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/board_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/board_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
```

What time standard is used by IIS as seen in the screenshot?

A. UTC
B. GMT
C. TAI
D. UT

Answer: A

NEW QUESTION 767
- (Exam Topic 2)
An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

A. Smurf
B. Ping of death
C. Fraggle
D. Nmap scan

Answer: B

NEW QUESTION 772
- (Exam Topic 2)
Where are files temporarily written in Unix when printing?

A. /usr/spool
B. /var/print
C. /spool
D. /var/spool

Answer: D

NEW QUESTION 777
- (Exam Topic 2)
Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

A. Accunetix
B. Nikto
C. Snort
D. Kismet

Answer: C

NEW QUESTION 781
- (Exam Topic 2)
Heather, a computer forensics investigator, is assisting a group of investigators working on a large computer fraud case involving over 20 people. These 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather responsibility is to find out how the accused people communicated between each other. She has searched their email and their computers and has not found any useful evidence. Heather then finds some possibly useful evidence under the desk of one of the accused.
In an envelope she finds a piece of plastic with numerous holes cut out of it. Heather then finds the same exact piece of plastic with holes at many of the other accused peoples desks. Heather believes that the 20 people involved in the case were using a cipher to send secret messages in between each other. What type of cipher was used by the accused in this case?

A. Grill cipher
B. Null cipher
C. Text semagram
D. Visual semagram

Answer: A

NEW QUESTION 785
- (Exam Topic 2)
Casey has acquired data from a hard disk in an open source acquisition format that allows her to generate compressed or uncompressed image files. What format did she use?
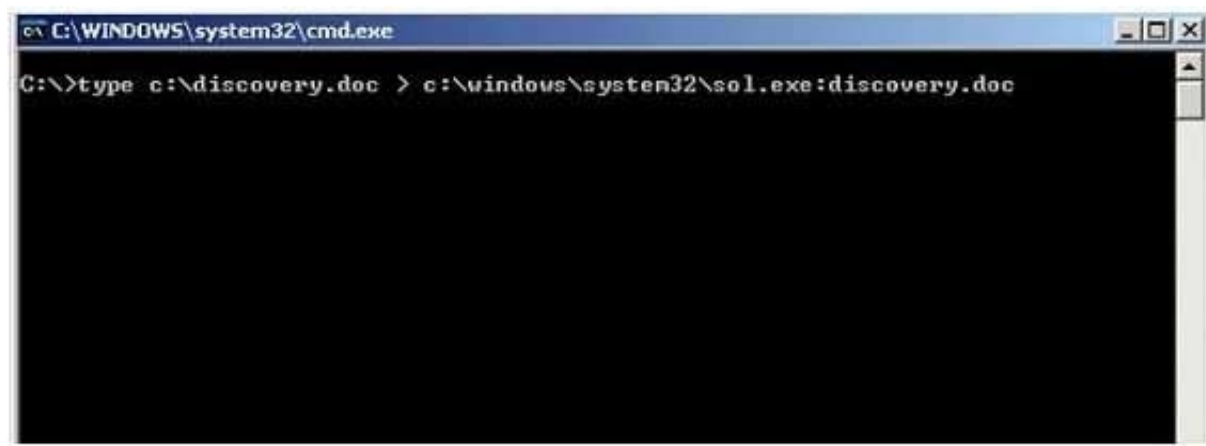
A. Portable Document Format
B. Advanced Forensics Format (AFF)
C. Proprietary Format
D. Raw Format

Answer: B

NEW QUESTION 788
- (Exam Topic 2)
What feature of Windows is the following command trying to utilize?

A. White space
B. AFS
C. ADS
D. Slack file

Answer: C

NEW QUESTION 791
- (Exam Topic 2)
Watson, a forensic investigator, is examining a copy of an ISO file stored in CDFS format. What type of evidence is this?

A. Data from a CD copied using Windows
B. Data from a CD copied using Mac-based system
C. Data from a DVD copied using Windows system
D. Data from a CD copied using Linux system

Answer: A

NEW QUESTION 795
- (Exam Topic 2)
How many possible sequence number combinations are there in TCP/IP protocol?

A. 1 billion
B. 320 billion
C. 4 billion
D. 32 million

Answer: C

NEW QUESTION 798
- (Exam Topic 2)
If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

A. Keep the device powered on
B. Turn off the device immediately
C. Remove the battery immediately
D. Remove any memory cards immediately

Answer: A

NEW QUESTION 801
- (Exam Topic 2)
Before performing a logical or physical search of a drive in Encase, what must be added to the program?

A. File signatures
B. Keywords
C. Hash sets
D. Bookmarks

Answer: B

NEW QUESTION 806
- (Exam Topic 2)
If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?

A. Lossful compression
B. Lossy compression
C. Lossless compression
D. Time-loss compression

Answer: B

NEW QUESTION 807

- (Exam Topic 2)

How often must a company keep log files for them to be admissible in a court of law?

A. All log files are admissible in court no matter their frequency
B. Weekly
C. Monthly
D. Continuously

Answer: D

NEW QUESTION 810

- (Exam Topic 2)

What is the smallest physical storage unit on a hard drive?

A. Track
B. Cluster
C. Sector
D. Platter

Answer: C

NEW QUESTION 815

- (Exam Topic 2)

Which of the following is an iOS Jailbreaking tool?

A. Kingo Android ROOT
B. Towelroot
C. One Click Root
D. Redsn0w

Answer: D

NEW QUESTION 818

- (Exam Topic 2)

Paraben Lockdown device uses which operating system to write hard drive data?

A. Mac OS
B. Red Hat
C. Unix
D. Windows

Answer: D

NEW QUESTION 819

- (Exam Topic 2)

Using Linux to carry out a forensics investigation, what would the following command accomplish? dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror

A. Search for disk errors within an image file
B. Backup a disk to an image file
C. Copy a partition to an image file
D. Restore a disk from an image file

Answer: D

NEW QUESTION 823

......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your 312-49v10 Exam with Our Prep Materials Via below:

https://www.certleader.com/312-49v10-dumps.html